UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF A GRAY JEEP CHEROKEE BEARING FL REG 24AUXR AND NINE CELLULAR DEVICES SEIZED ON MAY 3, 2024	)))))	**No.24-mj-**105-01-TSM **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Brian R. Gundersen of the Diplomatic Security Service (DSS), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the DSS, United States Department of State and have been sworn in this capacity since May 2009 after completing my training. In this role, I primarily investigate violations of federal statutes concerning visa and passport fraud, as well as identity crimes related to State Department programs. I am presently assigned to DSS's Portsmouth, New Hampshire resident office as a criminal investigator, where I specialize in investigations concerning passport fraud and identity theft. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer, I am authorized to execute warrants issued under the authority of the United States.

2. I received specialized training in law enforcement and criminal law from the Federal Law Enforcement Training Center in Glynco, Georgia and DSS's Training Facility in Dunn Loring, Virginia. I have conducted and participated in numerous investigations into various types of criminal violations, including passport and visa fraud, alien harboring, conspiracy, wire fraud, identity theft, and human trafficking offenses. Many of the cases I investigate are complex, international schemes involving the presentation of fraudulent identity

documents. During these investigations and others, I have analyzed fraudulent passports and fraudulent passport cards and have participated in the search and seizure of the aforementioned.

3. I received training on the use of electronic devices such as computers and mobile phones to further investigative efforts, and I have authored and executed multiple search warrants, to include search warrants on vehicles, residences, and electronic devices.

4. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C). *See* 28 C.F.R. §§ 60.1, 60.2, and 60.3; 22 U.S.C. § 2709. As a federal law enforcement officer, I am authorized to obtain and execute search warrants issued under the authority of the United States.

5. This affidavit sets forth facts and evidence that are relevant to the requested search warrant but does not set forth all of the facts and evidence that I have gathered during the course of the investigation of this matter. Rather, I have only set forth the facts that are necessary to establish probable cause to support the issuance of the search warrant. This affidavit is based on my own knowledge arising from my participation in this investigation, information provided to me by other law enforcement officers, including the Portsmouth Police Department (PPD), and my review of law enforcement reports related to this investigation. A portion of the information contained in this affidavit comes also from interviewing Kevin Dale DOWNS (DOWNS).

6. DOWNS is a sixty-six year old man and has an extensive criminal record in multiple states, including Florida, New Jersey, Tennessee, and Michigan, that dates back fifty years. DOWNS has used multiple social security numbers and aliases that are reflected on his criminal history. DOWNS has had multiple felony convictions for crimes that include theft offenses such as burglary, crimes related to a stolen property, check fraud, false report on a

police radio station, motor vehicle offenses as well as drug offenses including obtaining a controlled substance by fraud. It appears he may have a warrant for failure to appear in Indiana. Notwithstanding the Defendant's criminal history as well as his criminal involvement in this case, I found his post-arrest statement to be generally reliable during the course of his interview, which will be discussed later in this affidavit. Based on the investigation as detailed below, I believe DOWNS has committed several criminal offenses, including false use of a passport, aggravated identity fraud, and attempted bank fraud.

7. Based on the investigation as detailed below, I also believe the individuals identified as Anthony CUNNINGHAM (CUNNINGHAM), Lorraine NAAR (NAAR), and Paula STACK (STACK) are involved in conspiracy and aiding and abetting false use of a passport, aggravated identity fraud, and attempted bank fraud. It should also be noted that, at this time, we are still in the process of trying to verify if the identities of CUNNINGHAM, NAAR, STACK and Jasmyne REDMOND are, in fact, true names of the individuals who were stopped on May 3, 2024. For purposes of this affidavit, they will be referred to by these identifications.

STATUTORY AUTHORITY

8. 18 U.S.C. § 1543 provides, in pertinent part, that it is unlawful for any person to "willfully and knowingly use[], or attempt[] to use, or furnish[] to another for use any…false, forged, counterfeited, mutilated, or altered passport or instrument purporting to be a passport."

9. 18 U.S.C. § 1028(a)(1) provides, in pertinent part, that it is unlawful for any person to "knowingly and without lawful authority produce[] an identification document, authentication feature, or a false identification document" in relation to a circumstance described in 18 U.S.C. § 1028(c). 18 U.S.C. § 1028(c) describes several circumstances referred to in subsection (a), (c)(1) which reads as follows: "(1) the identification document, authentication

feature, or false identification document is or appears to be issued by or under the authority of the United States…"

10. 18 U.S.C. §1028A(a)(1) provides, in pertinent part, that it is unlawful for any person, "during and in relation to any felony enumerated in subsection (c), [to] knowingly transfer[], possess[], or use[], without lawful authority, a means of identification of another person." Subsection (c)(5) explicitly includes bank fraud and attempted bank fraud as a predicate felony for the offense of Aggravated Identity Fraud.

11. 18 U.S.C. § 1344 provides, in pertinent part, that it is unlawful for any person to "knowingly execute[], or attempt[] to execute, a scheme or artifice to defraud a financial institution or to obtain any of the moneys, funds assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises." 18 U.S.C. § 1349 criminalizes the attempt or conspiracy to commit bank fraud.

12. 18 U.S.C. § 20 (1) defines "financial institution" in pertinent part as "an insured depository institution (as defined in section 3(c)(2) of the Federal Deposit Insurance Act)." Bangor Savings Bank (BSB) is a Federal Deposit Insurance Corporation (FDIC) insured bank and therefore qualifies as a "financial institution" within the purview of 18 U.S.C. §§ 1344 & 1349.

13. Based on this training and experience and the facts set forth in this affidavit, I submit that there is probable cause to believe that the evidence and instrumentalities of criminal violations, including the following violations of 18 U.S.C. § 1543 (false use of a passport), 18 U.S.C. §§ 1028A(a)(1) (identity theft) and 1028A(a)(1) (aggravated identity theft), and 18 U.S.C. § 1344 & 1349 (attempted bank fraud) (collectively hereafter the "Subject Offenses"), as

well as aiding and abetting these Subject Offenses in violation of 18 U.S.C. § 2 and Conspiring to commit those Subject Offenses in violation of 18 U.S.C. §§ 371 or 1349. I believe that evidence and instrumentalities of these Subject Offenses as described in Attachment B are presently located within the property identified in Attachment A.

IDENTIFICATION OF THE PROPERTY TO BE SEARCHED

14. As further described in Attachment A, the property to be searched is as follows:

a. A dark grey 2020 Jeep Cherokee, bearing Florida registration 24AUXR, registered to PV Holdings, d/b/a Avis Rental (Target Vehicle);

b. A blue Samsung phone with no case assigned PPD Property No. 24-633-PR, recovered off the person of DOWNS (Device 1);

c. A black Motorola phone with no case assigned PPD Property No. 24-632-PR, recovered off the person of DOWNS (Device 2);

d. A white Apple iPhone with no case, broken back assigned PPD Property No. 24-631-PR, recovered from inside the TARGET VEHICLE in the front center console area between the area where CUNNINGHAM and NAAR were seated (Device 3);

e. A black Apple iPhone with no case assigned PPD Property No. 24-630-PR, recovered from inside the TARGET VEHICLE in the front driver's side door panel next to where CUNNINGHAM was seated (Device 4);

f. A white Apple iPhone with black Otterbox case assigned PPD Property No. 24-625-PR, recovered from inside of the TARGET VEHICLE and belonging to CUNNINGHAM who used this phone to look up an Avis rental agreement during the motor vehicle stop in the presence of PPD (Device 5);

g. A beige Apple iPhone with beige case assigned PPD Property No. 24-626-PR, recovered in the TARGET VEHICLE and belonging to NAAR, who was observed by PPD to be actively using this phone during the motor vehicle stop (Device 6);

h. A black Apple iPhone with no case assigned PPD Property No. 24-629-PR, recovered from inside the TARGET VEHICLE in the front center console area between the area where CUNNINGHAM and NAAR were seated (Device 7);

i. A black Samsung phone with red case assigned PPD Property No. 24-628-PR, recovered from inside the TARGET VEHICLE in the pocket behind the driver's seat, immediately in front of where STACK was seated (Device 8);

j. A white Apple iPhone with no case currently inside of the Target Vehicle on the front passenger seat where NAAR had been seated (Device 9);

hereinafter, Devices 1, 2, 3, 4, 5, 6, 7, 8, and 9 will be collectively referred to as "the Devices." PPD seized the Target Vehicle and the Devices on May 3, 2024, and the Target Vehicle and the Devices are currently located at the PPD, 3 Junkins Avenue, Portsmouth, NH 03801. The Target Vehicle and Devices are further described in Attachment A, which is incorporated herein by reference.

15. The requested warrant would authorize a search of the property described in Attachment A for the purpose of identifying both physical and digital evidence and instrumentalities, as particularly described in Attachment B.

PROBABLE CAUSE

BACKGROUND INFORMATION

16. DSS is investigating criminal activity related to and involving the creation and use of fraudulent United States passport cards in a scheme or schemes to use those cards for identification purposes to obtain money from bank accounts of victims at bank locations in the District of New Hampshire and elsewhere. Based on the investigation to date, I believe that the recent conduct in the District of New Hampshire discussed below is connected to similar offenses and conduct committed in the District of New Hampshire and may be connected to similar offenses and conduct committed elsewhere in the United States.

17. Based on my training and experience, as well as information I've obtained from other DSS agents engaged in similar investigations, I know that, at any given time, there are multiple fraud rings operating within the United States that utilize counterfeit passport cards to commit bank fraud and other offenses.

18. While the tactics utilized by these fraud rings are constantly evolving, I am aware of the following general practices of offenders involved in this type of conduct and conspiracies to commit such conduct.

19. Offenders obtain personal identifying information (PII) and bank account information for a real victim. Offenders commonly obtain such information by stealing mail and/or checks and purchasing such information from the web, messaging services, or the so-called Dark Web.

20. After obtaining such information, offenders forge, counterfeit, and falsely make—or purchase forged, counterfeited, and falsely made—a United States passport card, a state driver's license, or a state identification card bearing the name and identifying information of their victim.

21. Offenders also create counterfeit bank cards for their victim's account or in their victim's name for other accounts, either real or fictional. Offenders often seek to use such cards as an additional form of identification.

22. Offenders recruit individuals to enter the victim's bank and attempt to withdraw money from the victim's accounts using the counterfeit passport card, state driver's license, or state identification card as a form of identification. A photograph of this impostor who enters the bank is placed on the counterfeit passport card, license, or identification card along with the victim's identifying information. Offenders often compensate such impostors with drugs, money, or both. I know that many of the larger organizations or rings engaging in this type of conspiracy have ties to—or are directly involved in—drug trafficking and other criminal offenses.

23. Before the impostor enters the bank, they or their associates often contact the bank to obtain victim's account balance, frequently by calling the bank. Offenders also frequently share the victim's PII with the impostor in electronic form for the impostor to learn in order to successfully impersonate the victim.

24. Some banks permit an account holder to utilize two-factor authentication, such as receiving a one-time code via phone call or text message to the account holder's mobile phone to confirm their identity. Offenders often use a process known as "SIM swapping" to take over the phone number of their victim and bypass such two-factor authentication. SIM swapping often involves creating a Subscriber Identity Module ("SIM card") containing the identifiers used to authenticate the victim's mobile telephone to their service provider's network, allowing offenders to receive one-time security codes sent by the victim's bank to the victim's mobile telephone number.

25. Once inside the bank, the impostor presents the counterfeit passport card, driver's license, or identification card bearing the impostor's image and the victim's name and other identifying information in order to withdraw money from the victim's bank account. The impostor often presents the counterfeit bank card in the victim's name as a second form of identification. If the impostor is successful in withdrawing money from that bank account, the impostor frequently travels to another branch of the same bank to attempt to withdraw additional money from the same account. The impostor typically continues in this fashion until they are unsuccessful in withdrawing additional money from the account. I am aware of several instances in which impostors have traveled to additional branches of the same bank even when they are unsuccessful at withdrawing money from the victim's account.

26. Imposters will often times use multiple electronic devices to assist them in carrying out their impersonation, including the use of cell phones and Bluetooth headsets. Imposters will use these electronic devices while communicating with bank staff to clandestinely record and communicate with co-conspirators who may feed information or other tips to assist in the deception to the imposter over the phone, by way of telephone call or electronic message.

27. Offenders typically seek to use counterfeit United States passport cards because of the belief that banks will accept federal identification without requiring a second form of identification, whereas banks often request additional forms of identification from individuals who present an out-of-state identification card.

28. Money withdrawn or transferred from a victim's account is typically laundered in some form to prevent—or attempt to prevent—law enforcement from tracking and identifying the proceeds of the criminal conduct.

INITIAL RESPONSE ON MAY 3, 2024

29. On May 3, 2024, at approximately 2:34 PM PPD responded to BSB, which is located at 2400 Lafayette Boulevard, Portsmouth, New Hampshire, for a report that a homeless male was at BSB attempting to cash a check utilizing fake identity documents. The male was described as wearing a green hat, black coat and jeans, and was last seen in the parking lot outside of the bank.

30. According to BSB staff, DOWNS entered BSB and attempted to cash a $7,400.00 check made payable to Victim One. DOWNS produced a U.S. Department of Veterans Affairs (VA) card and passport card in the name of Victim One to a staff member in an attempt to validate his identity. DOWNS was able to recall PII about Victim One, specifically Victim One's true date of birth and the true name of the wife of Victim One. DOWNS also wrote down the correct social security number of Victim One.

31. Victim One is a real customer of BSB and is an account-holder at BSB.

32. BSB staff observed that DOWNS was holding a phone by his side while interacting with the teller and believed he may have been communication with someone while speaking with the teller. BSB staff informed responding PPD officers that earlier in the day, an unidentified male had attempted to make a fraudulent withdrawal at the BSB branch located at 8 Bow Street, Portsmouth, NH 03801.

33. The teller denied the transaction, and the male left the bank.

34. A responding PPD officer, Alex McMillen, encountered an individual matching the suspect's description walking away from the bank in the same plaza and subsequently identified him as DOWNS.

35. Officer McMillen asked DOWNS if he had just attempted to cash a check at BSB and he said he was in there talking to a teller. Officer McMillen asked if he still had the check in his possession, and DOWNS stated the bank held it. Officer McMillen asked DOWNS for identification, and DOWNS provided a Veteran Affairs card in the name of Victim One printed on it. Officer McMillen asked DOWNS for his date of birth and social security number. DOWNS provided Victim One's date of birth and stated that he could not remember his social security number due to a head injury. Officer McMillen asked if he had any other identification documents on him and he initially said no. While another PPD officer was speaking with DOWNS, DOWNS produced the check in question made out to Victim One in the amount of $7,400. DOWNS stated that he is a veteran and that he recently sold a vehicle in Georgia and that he was cashing the check to buy a replacement vehicle.

36. PPD asked DOWNS how he got to the bank, and DOWNS stated that his wife "Sharon" had dropped him off and that he was looking for her vehicle. Officer McMillen explained to DOWNS that he is familiar with organizations that transport homeless people from out of state to cash stolen checks for drugs as payment. DOWNS immediately uttered that he was picked up in Michigan by a crew who told him they would give him fentanyl in exchange for cashing checks. DOWNS produced a United States passport card #c812673426 with his picture and Victim One's information. DOWNS stated he was also provided with this card by the crew as a second form of identification.

37. Both of the identity documents contained photographs bearing DOWNS' image, accompanied with Victim One's name. These are believed to be the same identification cards as he produced minutes earlier at BSB.

38. DOWNS stated that he was picked up in Michigan by a car of black males who transported him to New Jersey. At one point, DOWNS described the car that dropped him off as a grey Jeep, possibly with NY license plates. DOWNS stated that the group rented a motel room for him in New Jersey, gave him clothes to wear, and gave instructions on how to cash the checks. DOWNS stated that the group kept him "stoned," which I understood to mean high on drugs, and also stated that the group would pay for prostitutes while at the motel.

39. Officer McMillen asked DOWNS if the crew that dropped him off had provided him with a cell phone, and DOWNS stated that they did, and DOWNS produced Device 1, which was in his pocket. DOWNS also stated that he had a personal cell phone on his person, which was identified by PPD officers as Device 2. DOWNS was asked if the people who had dropped him of held his actual ID and he said no. PPD asked DOWNS if he had Victim One's information written down, and he said that it was on the phone. DOWNS explained that he holds the phone at his side while conducting transactions to read the information.

40. Simultaneously, PPD Patrol Officer Ian Efstathiou responded to the vicinity of the BSB. From his training and experience, Officer Efstathiou knows that these types of financial crimes are typically carried out by multiple individuals working together and often involve "handlers" who are located in nearby vehicles. In addition, recent law enforcement reporting indicates that these vehicles are typically rental cars and sport utility vehicles.

41. While pulling into the area of 2400 Lafayette Road, Officer Efstathiou observed the Target Vehicle exiting the north side of the bank parking lot. Officer Efstathiou observed that the Target Vehicle had no front license plate and a toll transponder box on the windshield, which is consistent with those used by car rental companies. Officer Efstathiou pulled behind the Target Vehicle and observed rear Florida license plate 24AUXR.

42. While Officer McMillen was out with DOWNS, Officer Efstathiou radioed dispatch that he had followed this vehicle onto Lafayette Road that appeared to be coming from the bank. Officer McMillen asked DOWNS if this was the vehicle he was waiting to be picked up by, and DOWNS said yes. DOWNS stated the he believed there were two black males and a white female in the vehicle. DOWNS was unable to provide further description of the individuals, again blaming his head injury. Officer McMillen asked if he knew the names of the occupants and DOWNS stated "Antonio" and "Dre."

43. Officer McMillen asked for DOWNS' real name and date of birth, and he provided the name of "Kevin D. Brown" with a DOB of 11/17/1956 with residency in Michigan. Officer McMillen had dispatch run that information and did not locate any driver's license or criminal history associated with that identification, suggesting that the identification may be false. DOWNS then changed his DOB to 11/16/1956. Officer McMillen was unable to positively identify DOWNS roadside. While another officer stayed with DOWNS, Officer McMillen went into the bank to interview the staff. After learning what had occurred inside of the bank, Officer McMillen returned to the area where DOWNS was and placed him under arrest for related state charges. While handcuffing DOWNS, Officer McMillen noted he was wearing a black wrist brace under the long sleeve of his jacket. Officer McMillen asked if he was injured, and DOWNS stated that he was given the brace by the crew that dropped him off and told him he could use it as an excuse on why the signature doesn't match the one on file with the bank.

44. PPD seized Devices 1 and 2, the $7,400 check payable to Victim One, as well as the U.S. passport card and VA card bearing Victim One's name.

45. A search incident to arrest of DOWNS revealed an envelope zippered into the lining of his leather jacket. PPD asked DOWNS what it was, and DOWNS replied that it was his life

savings. The envelope contained $7,400 in one hundred dollar bills. Also located was a Georgia driver's license bearing DOWNS' image with the name of Victim Two printed on it, as well as another check made out to Victim Three for $2,550. PPD seized the cash, the identification document for Victim Two and the check made payable to Victim Three.

46. DOWNS provided several false social security numbers as police attempted to identify him for the booking process. DOWNS requested to speak with a detective.

47. A PPD detective responded to the booking room and was given DOWNS' true name and date of birth. DOWNS was given his *Miranda* warnings and spoke with Detectives in an interview room.

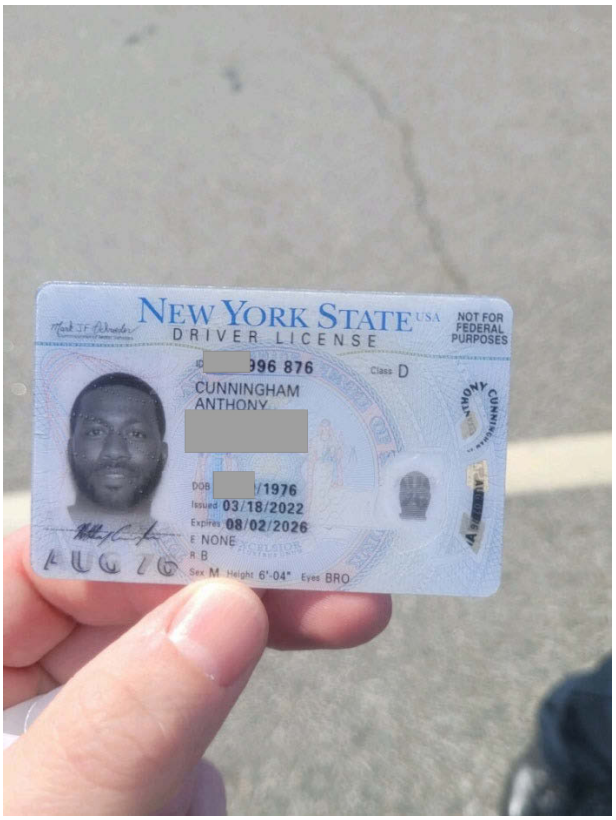
48. Following the interview, DOWNS was processed, fingerprinted and photographed.

THE MOTOR VEHICLE STOP OF THE TARGET VEHICLE

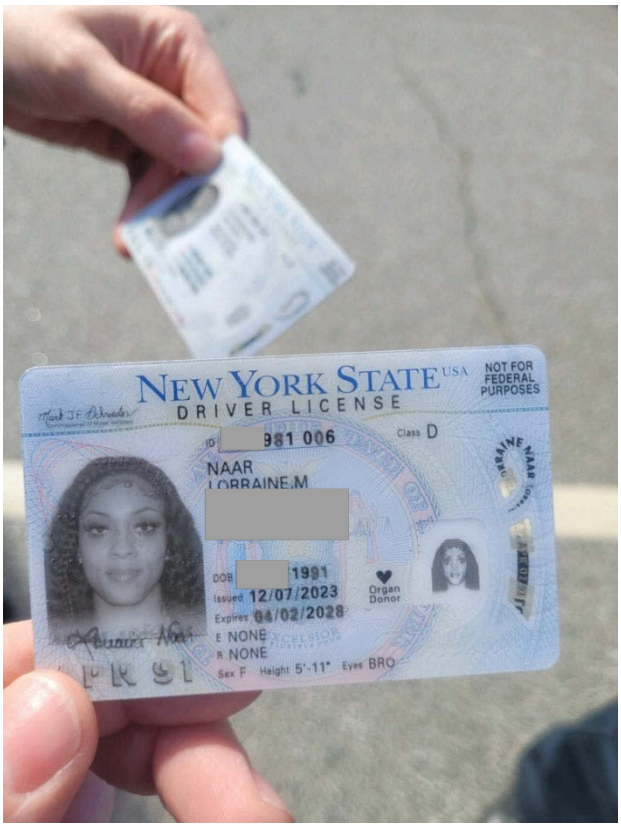
49. Also on May 3, 2024, at approximately 2:35pm, Officer Efstathiou observed the Target Vehicle exiting the parking lot of BSB. Officer Efstathiou observed that he observed the vehicle put on its left turn signal and then travel abruptly from the outside to the inside travel lane, causing traffic to shift to avoid it. Officer Efstathiou initiated a traffic stop in the vicinity of 3611 Lafayette Road, Portsmouth, NH for the civil traffic infraction of RSA 265:45, "Turning Movements and Required Signals." The driver of this vehicle was ultimately given a verbal warning for this traffic infraction. Officer Efstathiou made contact with the driver of the Target Vehicle, advised the driver of the reason for the stop and requested the driver's license and registration. The driver identified himself by producing a New York drivers license in the name of CUNNINGHAM as well as a receipt from Avis Car Rental. During the interaction with CUNNINGHAM, Officer Efstathiou noted that he appeared nervous and constantly moved his hands from his thighs to the center console and a sling bag located on the center console, touching

it repeatedly. He continued to fidget with his wallet and made several attempts to hand the Officer an American Express card after handing him his license. A review of the rental agreement indicated that the car was originally rented in CUNNINGHAM's name from LaGuardia International Airport from April 18, 2024 through May 2, 2024.

50. PPD later took a photograph of the driver identified as CUNNINGHAM as well as a copy of the license he provided, and those photographs are attached below:



51. Officer Efstathiou observed a female passenger in the front passenger seat, who provided a New York driver's license in the name of NAAR. PPD later took a photograph of the front seat passenger identified as NAAR as well as a copy of the license she provided, and those photographs are attached on the following page:



52. Officer Efstathiou observed a female in the second row rear passenger seat, seated directly behind the driver with her back to the window, who identified herself as STACK. STACK was unable to provide identification to police, however she stated that her identification was issued by the state of Arizona and that her address is in Texas. STACK further indicated that she did not know the driver, but that she was friends with NAAR. Officer Efstathiou requested PPD dispatch attempt to locate photographs of STACK to verify her identity. PPD dispatch was unable to locate an identification for STACK in Arizona, but PPD dispatch did obtain a confirmation of an identification for STACK in Texas; however, the Texas identification for STACK did not have a photograph of STACK available, therefore STACK's identification could not be verified. PPD later took a photograph of the rear seat passenger identified as STACK that is attached on the following page:

53. CUNNINGHAM told Officer Efstathiou that the vehicle contained three occupants and that they were coming from "around here."

54. At the same time, NAAR spoke over CUNNINGHAM and stated that the group was visiting with family in Maine. NAAR stated that they had gone out to get seafood because STACK could not get fresh seafood in Arizona. While Officer Efstathiou spoke with CUNNINGHAM, NAAR repeatedly continued to speak over him. The occupants claimed to be traveling back to Maine after having gotten lobster and were lost. NAAR claimed to be using GPS but also having been on the phone and not paying attention to their directions.

55. While completing law enforcement database checks of the vehicle occupants, Officer Efstathiou received information from PPD officers that DOWNS had provided a description of the vehicle that transported him to the BSB as a gray Jeep possibly with New York

license plates, which was consistent with the Target Vehicle. DOWNS also stated to PPD officers that he had seen a firearm and that it may be in the vehicle.

56. Officer Efstathiou approached the Target Vehicle and used his flashlight to illuminate the rearmost section of the interior through the tinted windows, where he observed what appeared to be a person wearing dark clothing, curled up between the second and third row seat. Since CUNNINGHAM stated that the vehicle only had three occupants, and based on DOWNS' information that it may contain a firearm, Officer Efstathiou opened the rear passenger door.

57. Officer Efstathiou verbally addressed the fourth occupant, who sat up and verbally identified herself as REDMOND of Atlanta, GA. REDMOND put her hands up and said she was "just sleeping." REDMOND stated that she did not have identification on her person. Officer Efstathiou requested PPD dispatch attempt to locate photographs of REDMOND in an attempt to confirm her identity. PPD dispatch was able to locate identification records for REDMOND out of Georgia, however, the Georgia identification for REDMOND did not have a photograph of REDMOND available. Therefore, the identifications of REDMOND could not be verified with the information that was provided. PPD later took a photograph of the second rear seat passenger identified as REDMOND that is attached on the following page:

58. For officer safety, all four occupants were individually escorted from the vehicle, frisked for weapons, and then seated along the shoulder of the roadway.

59. CUNNINGHAM now stated that the group was on their way back to New York, and not Maine. CUNNINGHAM was informed that the lease of the vehicle had expired on May 2, 2024; CUNNINGHAM stated that he renewed the agreement and was permitted to use his phone, Device 5, to look up the renewed contract. CUNNINGHAM showed PPD a renewed contract through May 7, 2024. Device 5 was then placed back inside the Target Vehicle.

60. REDMOND stated that they had gone into the shopping plaza to get Chipotle and that she had fallen asleep after a long drive and was unaware that the vehicle had been pulled over. Officer Efstathiou noted that this statement was unusual because there was a Chipotle business inside of the plaza where the BSB was located, and only approximately three minutes had passed from the time that he initially observed the vehicle leave the BSB parking lot to the time that he stopped the vehicle.

61. PPD showed the photographs of the four occupants of the Target Vehicle to DOWNS. Upon viewing the photographs of the four occupants from the Target Vehicle, DOWNS confirmed that all four occupants were the individuals that he had been traveling with in furtherance of the check-cashing scheme. According to the report of Officer Efstathiou, DOWNS further stated that the Target Vehicle contained illicit drugs, as well as money that they had obtained through previous illegal activity.

62. Based on the inconsistencies of the information provided by the Target Vehicle occupants, as well as the information provided by DOWNS that the vehicle occupants were involved in the fraud and that they used cellular phones to communicate in furtherance of the conspiracy to defraud banks, Officer Efstathiou seized the vehicle and its' contents, as well as all cell phones,[1] namely Devices 3, 4, 5, 6, 7, 8, and 9.

63. PPD recovered Devices 3 and 7 from the front center console area of the Target Vehicle in between where CUNNINGHAM and NAAR had been seated;

64. PPD recovered Device 4 from the front driver's side door panel of the Target Vehicle, next to where CUNNINGHAM had been seated;

[1] It is worth noting that REDMOND identified a black Apple iPhone with purple case assigned PPD Property No. 24-627-PR, recovered from inside of the TARGET VEHICLE and belonging to REDMOND who verbally indicated to PPD that it was her phone during the motor vehicle stop. Although this device was initially seized by police, this warrant is not requesting search and seizure of that device at this time.

65. CUNNINGHAM used Device 5 during the motor vehicle stop and in PPD presence to look up the extended lease agreement, before it was placed back inside of the Target Vehicle, where it was later recovered by PPD;

66. PPD observed NAAR actively using Device 6 during the motor vehicle stop and it too was recovered from inside of the Target Vehicle.

67. PPD recovered Device 8 from the rear seat pocket of the driver's seat, which was immediately in front of the area where STACK was seated within the Target Vehicle;

68. PPD observed Device 9, which is still currently inside the Target Vehicle on the front passenger seat where NAAR was seated.

69. The occupants in the vehicle were given the opportunity to request any specific items from the vehicle, to include identification, limited credit cards in their names and warmer clothing, in order to continue their travel. They were then provided courtesy escort to the C&J Trailways station located at 185 Grafton Drive in Portsmouth, New Hampshire.

70. Devices 3, 4, 5, 6, 7, 8, and 9 all remained in the Target Vehicle for the duration of the stop, however, as previously noted, CUNNINGHAM had been given his cellphone, Device 5, in an attempt to locate a more current rental agreement as previously described. His phone, Device 5, was then returned to the Target Vehicle.

71. Due to the sensitive nature of the data on cellphones and their ability to be remotely accessed and have information deleted, all cellphones in plain view were removed from the vehicle and properly secured. PPD removed Devices 3, 4, 5, 6, 7, and 8, from the Target Vehicle. Device 9 remained in the Target Vehicle. Of the seven devices removed from the vehicle, Devices 3 and 4 were off; the remaining Devices were either placed into airplane mode, or placed into a faraday box if they could not be placed into airplane mode, in order to preserve their contents.

72. Based upon my training and experience, I know that turning a phone off or placing it into airplane mode will prevent users from remotely wiping or altering the data contained on the phone. Based on my training and experience, I am aware that "faraday boxes" are storage devices that block most major signals—such as wireless, Bluetooth, and most cellular connections—from reaching a cellular device. By storing a cellular device in such a box, it is possible to prevent an individual from remotely clearing, wiping, or resetting a device before law enforcement can search the device to review and/or seize its contents.

73. The phones were then transported back to PPD and entered into evidence in a secure cell phone storage area. The phones that remained on were plugged into chargers to maintain their power status.

74. A tow truck arrived and towed the Target Vehicle to the PPD secure parking lot in Garage Bay 3. The doors of the Target Vehicle were locked, and evidence tape was applied to all of the doors, windows, hood, trunk and fuel door. The tape was then initialed, dated, and photographed to document the condition of the Target Vehicle.

INTERVIEW OF DOWNS

75. On May 3, 2024, at approximately 4:30 PM, I received a call from the PPD shift commander and responded to the PPD to interview DOWNS. I identified myself as a Special Agent with DSS and verbally read DOWNS his *Miranda* rights. DOWNS verbally agreed to understanding his *Miranda* rights and consented to participating in an interview, which was audio and video recorded by the PPD.

76. In sum and substance, DOWNS stated that he has been participating in "bank work" for approximately two years, after being picked up off the street in Orlando, Florida by New York gang members known as "Rockstar" and "Jigga Hustle". From my training and experience, I

understood the term "bank work" to refer to identity theft and acts of attempted or completed bank fraud.

77. When asked specifically what kind of work he did for the group, DOWNS stated "scott work." From my training and experience, I know that "scott work" refers to individuals who utilize counterfeit passport cards and identity documents to commit bank fraud and other offenses. The individuals who actually enter the bank refer to themselves as "Scotties." DOWNS stated that his handlers give him IDs with his picture on it, as well as account information, and that he goes into the bank to "try to pull the money out," which I understood to mean withdraw funds from legitimate customer's bank accounts that do not belong to DOWNS.

78. When asked how the group obtained account and victim information, DOWNS stated some of it was done through "fishing" and breaking into mailboxes. DOWNS stated that the groups use a "tree service" and bank checks to obtain the initial account information. This information includes victim names, addresses and account numbers. The group then provides this preliminary information to a "lookup guy" who conducts deeper background checks to obtain driver's license and social security numbers.

79. DOWNS stated that when his handlers, to include NAAR, send him into a bank, his handlers send him a background check, specifically from the website People Finder, which includes the victim's social security number, phone numbers and addresses. DOWNS is also given a check, which will be cashed against the victim's account, which DOWNS referred to as "cash against". DOWNS stated that these procedures were followed for his attempted withdrawals at the BSB.

80. At approximately 6:00 am on May 3, 2024, DOWNS stated that he left the Bronx, New York, that morning with "Lorraine" and "Antonio," referring to NAAR and

CUNNINGHAM, respectively. DOWNS later explained in the interview that STACK and REDMOND also came from and live in the same motel in New York. When the group left New York, they travelled in the vehicle "they just got," referring to the Target Vehicle stopped by the PPD. DOWNS further descried the Target Vehicle as a black Jeep.

81. DOWNS admitted to entering two BSB branches, recalling that the identity he used at both branches was for Victim One, and commenting that he got caught at the second branch. This statement was consistent with the information that was relayed to PPD by BSB regarding an earlier attempted bank fraud at another BSB location. DOWNS stated that he was purposely unsuccessful in his attempts to withdraw money because he is an active confidential informant with the Grand Rapids, Michigan police department, therefore he can't commit "too many felonies."[2]

82. DOWNS stated that if he is successful in withdrawing money from a bank, he gives the proceeds to his handlers. DOWNS estimates that his handlers make approximately $15,000 to $30,000 per day. DOWNS also stated that money is "in the car, you should've found money in the car today."

83. DOWNS identified the producer of the counterfeit identity documents as "Tay" and admitted to visiting Tay's apartment, located in the Bronx, New York, on May 2, 2024 to pick up the "I's[3]" that NAAR had ordered. DOWNS stated that NAARS pays approximately $250 for each identity. DOWNS waited in the front room for approximately six hours until the group was called up by Tay to take possession of what DOWNS described as the "IDs you guys got right

[2] In the days after this interview, I reached out to the Grand Rapids, Michigan police department and was able to confirm with them that DOWNS was a reliable confidential informant for them from 2019 through 2023. His work as a confidential informant was terminated in 2023 due to picking up new identity fraud related charges stemming from an 8/23/2023 arrest in Knox County, Tennessee. A review of Knox County Sheriff's Office report #2308231704 indicates that DOWNS was found in possession of 12 fraudulent passport cards bearing his image. DOWNS was charged with identity theft, identity theft trafficking and theft of property.

[3] "I's" is street slang for stolen identities.

now," which I understood to refer to the documents previously in DOWNS' possession that were seized by the PPD. DOWNS described the IDs as driver's licenses, U.S. passport cards, VA cards and credit cards. DOWNS observed Tay hand these items to NARR.

84. DOWNS stated that NAAR is the boss of their crew and is a highly ranked member of a Dominican Republic gang located in the Bronx, New York. NAAR is saved as the contact named "Boss Lady" in DOWNS' cell phone contact list, and also uses the "Boss Lady" username on the Telegram messenger application, which he uses to communicate with her regarding bank fraud schemes.

85. DOWNS also stated that CUNNINGHAM is highly ranked within a Jamaican gang, which is also based in the Bronx, New York. According to DOWNS, both NAAR and CUNNINGHAM are heavily involved in narcotics and gun trafficking, as well as identity theft.

86. DOWNS identified STACK as another "scottie" that he works with. DOWNS stated "they got another scott in the car," referring to the Target Vehicle. When asked who, Downs replied, "Paula," referring to STACK. When asked if STACK went into any banks today, DOWNS responded, "yea, she went into two," which he identified as a Kennebunk[4] bank, unknown location. DOWNS believes STACK was successful in her attempts to withdraw money, however he implied that his handlers often isolate Scotties from each other to limit information. DOWNS added that STACK would have told him if she was successful in the bank when they returned to their motel, which is located in New York. DOWNS indicated that STACK has her own room at the motel.

87. DOWNS identified REDMOND as his "girlfriend," who he met in Atlanta, Georgia. DOWNS stated he has been dating REDMOND for the past month. DOWNS stated that REDMOND only accompanies him on these trips, and that REDMOND does not participate in

[4] In the days after this interview, I have developed information that STACK attempted to withdraw $7,400 from the Kennebunk Savings Bank, which is located at 111 Maplewood Ave, Portsmouth, NH 03801.

bank work. DOWNS added that his handlers can hold his relationship with REDMOND over his head because "they got my girl." DOWNS stated that he shares a room at the motel in New York with REDMOND.

88. DOWNS stated that over the past two years he has defrauded banks in multiple states,[5] including Texas, Tennessee, Kentucky, Florida, Maryland, Delaware, North Carolina, South Carolina, Michigan, Ohio, Indiana and New Hampshire, at the direction of NAAR. DOWNS estimated that he has personally stolen $1.2 million, which he turns over to NAAR and "Lamar," which is the father of NAAR's child.

89. DOWNS stated that his phones and the phones of his travelling companions contain extensive evidence of identity theft and bank fraud. Specifically, DOWNS stated that the "phone they gave me, they left so much stuff on there man, I'm talking about ID information, check pictures, bank information, the whole thing, they left it all on there." What I understood this to mean was that DOWNS was stating that on the phone that his handlers provided to him, there is evidence of the Subject Offenses, including identification information of victims, photographs of checks, bank information, and other details needed to carry out the criminal scheme. DOWNS stated during his interview "look on Telegram, under Boss Lady or under Johnny Walker, that's another boss." DOWNS identified "Johnny Walker," true name unknown, as another individual in a leadership position. DOWNS stated that "Johnny Walker" accused DOWNS of withholding proceeds, which resulting in an assault against DOWNS.

90. It should be noted that DOWNS also provided verbal consent to search his devices, Devices 1 and 2, during this interview, and this consent was audio- and video-recorded. DOWNS

[5] In the days after this interview, I have developed information that DOWNS has also committed bank fraud in Massachusetts on April 26, 2024, which was not a state that DOWNS named in his interview.

stated that information related to criminal activity could be found on both Devices 1 and 2, the "majority" of which would be on Device 1.

91. On Wednesday, May 8, 2024, I conducted visual observation of Devices 1 and 2 based on this consent, where I observed photos of DOWNS with what appear to be narcotics and money, as well as references in text messages about "scott work" and being a "scottie;" However, much of the data would not populate, and I understand that this may be data related to the encrypted application Telegram, which DOWNS stated that he used to communicate with his co-conspirators and handlers. Based on my training and experience and the training and experience of other officers, I understand that Telegram may need to be connected to a network in order to download the data associated with it, and therefore at this time we do not have the capacity locally to download Devices 1 and 2 in a manner that would show communications on Telegram. Therefore, I would respectfully request a warrant to continue the search of Devices 1 and 2 by sending them to a lab in Washington D.C. where they can be downloaded with a program that allows for the viewing of Telegram data. To my knowledge and as of the date of submitting this warrant, DOWNS has not revoked consent; therefore, the application for the warrant for Devices 1 and 2 is sought out of an abundance of caution.

92. DOWNS indicated that the group mostly uses Telegram to buy and trade identities. DOWNS stated that NAAR provided him with a cell phone to communicate with her when he got out of jail in Georgia, which would have been approximately January 2024 according to his record. DOWNS stated that he got the phone from NAAR in Atlanta, and subsequently met REDMOND in Atlanta. DOWNS stated that NAAR conducts background checks on potential victims, using People Finder, in order to obtain additional PII about them.

93. DOWNS stated that he is presently living at the Budget Motor Inn, 87 S. Liberty Drive, Stony Point, New York, which he described as a "scottie spot," which I understood to mean a place where individuals who participate in identity theft and bank fraud live together. NAAR pays DOWNS' rent at the Budget Motor Inn, which is $80 per day.

CONSULAR DATABASE RECORDS

94. A subsequent query of the Department of State Consolidated Consular Database (CCD) for passport card #c812673426 found no records. Based on my training and experience, I know that this proves that the passport card that DOWNS possessed with the name of Victim One was a counterfeit passport card. CCD identified two passport records for Victim One, but neither of which were for passport cards. In addition, the individual depicted in the Victim One passport records is different than DOWNS, who is the individual depicted in the counterfeit passport card #c812673426, which was found on DOWNS.

95. Attempts have been made to contact Victim One. The Fraud department of BSB has confirmed that Victim One is a real customer of their bank. BSB made contact with Victim One's wife, who stated that Victim One is currently traveling outside the state. Victim One has yet to return my call, but I believe he is a real person for purposes of Aggravated Identity Fraud.

96. Therefore, I believe that there is probable cause that DOWNS has committed and is committing the Subject Offenses and that evidence and instrumentalities of these Subject Offenses will be found from searching the Target Vehicle and the Devices.

TRAINING & EXPERIENCE RELATED TO ITEMS TO BE SEARCHED FOR

97. *Controlled Substances and Weapons:* Based upon the statement of DOWNS, where he indicated that he was compensated in illicit narcotics and that he has seen firearms in the Target Vehicle in the past, I believe that evidence of narcotics and firearms may exist within the

vehicle. Based upon my training and experience, I know firearms and other weapons are tools of the drug trade and other illicit businesses, often used by criminals who are looking to protect their narcotics or criminal proceeds from would-be robbers, where they would be unable to report any robberies of illicit substances or income to the authorities without criminal exposure. I would therefore request to search for controlled substances as well as any weapons to include firearms, ammunition, rifles, shotguns, privately manufactured firearms, explosive devices, silencers, magazines, Glock switches, targets, ballistic vests, etc., in which there is no immediate appearance of legitimate use or lawful possession.

98. *Any Identifications or PII:* Based upon my training and experience, as well as the collective knowledge and experience of other agents and in my office, I am aware that individuals involved in identity theft and financial fraud often store identity documents, PII, and other tools of their trade in their homes, hotel rooms, automobiles, garages or outbuildings on their properties, basements, or on their electronic devices, or other places under their immediate control. I am aware that it is generally a common practice for imposters to store their identity documents and related paraphernalia in automobiles, electronic devices, or other locations they access with frequency. I am aware that PII may be recorded in writing and electronically, in written communications such as email, text or other social media platform, photographs, video and voice messages.

99. *Electronic Devices*: Based upon my training and experience as previously described, as well as the statements of DOWNS that he was provided a cell phone by the leaders of the organization and used it to communicate in furtherance of the Subject Offenses, coupled with the large number of cell phones located within the vehicle (particularly the number of cell phones that are attributable to the alleged leaders of the conspiracy, CUNNINGHAM and NAAR),

I believe this organization was using electronic and cellular devices to communicate with each other and in furtherance of their criminal conspiracy and scheme to defraud. Based on my training and experience, I know that individuals involved in identity theft and financial fraud typically use electronic and/or cellular devices in order to facilitate financial frauds, including to order and take orders for counterfeit identity documents or to set up shipments. I am aware that items such as cell phones, pagers, and other electronic devices, as well as U.S. currency, are often located in automobiles or on an individual's person.

100. *Longevity of Documents and Records in General*: Based upon my training and experience, there are a number of different kinds of records or documents that may be maintained physically or electronically that may contain evidence of the Subject Offenses. Based upon my training and experience, these records are durable, meaning they often survive over long periods of time. There are many reasons why an individual will generally maintain records for long periods of time. One reason is that the records will often seem innocuous because of their nature (e.g. financial, credit card and banking documents, travel documents, receipts, client lists, documents reflecting purchases of assets, personal calendars, telephone and address directories, check books, videotapes and photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone bills, keys to safe deposit boxes, packaging materials, computer hardware and software). Second, the individual may no longer realize he/she still possesses the records or may believe law enforcement could not obtain a search warrant to seize the evidence. Lastly, it is common for individuals to set aside or store such records, and because they generally have no immediate need for the records, they are often forgotten. To law enforcement, however, all these items may have significance and relevance when considered in

light of other evidence. The following are descriptions of records and documents which may contain evidence related to the Subject Offenses:

a. *Identity Records:* Based on my training and experience, individuals involved in identity theft will commonly maintain records and documents pertaining to the possession, purchase, sale, manufacture, or disposition of fraudulent identification documents, to include those obtained through fraud or those manufactured, altered, or generated in digital form. In addition, individuals involved in identity fraud will commonly retain true or counterfeited Government-issued documents, to include passports, visas, driver's licenses, certificates, Social Security cards, or any other indicia of identity or citizenship.

b. *Travel Records:* Based on my training and experience, individuals involved in identity theft will travel all over the country to commit fraud at different branches of banks within the United States, and often times these individuals retain records of air, sea, or ground travel into or within the United States, including receipts, boarding passes, airline or other carrier documentation, hotel records, hotel keys, invoices, photographs, visas, visa supporting documents or digital copies thereof. By changing their geographical location, these individuals make it harder for law enforcement to track the fraudsters down and identify patterns of criminal conduct. These records and documents of travel may show the locations of different historical and future identity fraud scheme plans.

c. *Financial Records:* Based on my training and experience, individuals involved in identity theft and financial fraud will commonly maintain records and documents which provide a paper trail for money laundering of illicit financial fraud proceeds,

often long after the actual transactions. In addition, banking and financial records of any kind may be useful information in an identity fraud investigation to show where money is coming from (e.g. a victim account) or going to (e.g. a suspect account). Additionally, financial records such as books, records, ledgers, journals, statements, receipts, invoices, billings, financial statements, balance sheets, notes and work papers concerning DOWNS, CUNNINGHAM, NAAR, STACK and REDMOND, and any other names that they may be known by, and any business entities in which they are stakeholders, or co-conspirators may be useful in showing where the illicit proceeds go and paint a picture of the conspirators' financial relationship. Documents evidencing expenditures of identity theft and bank fraud proceeds including, the purchase of large assets, including digital image storage devices, records of real estate or securities transactions, escrow files, wire transfer records, automobiles, motorcycles, trucks, or other vehicles purchased with cash or cash equivalents; credit and debit card records, including records of purchases, withdrawals, deposits and cash advances made with credit and debit cards, and including statements and receipts.

d. *Photographic Records*: Based on my training and experience, individuals involved in identity theft and financial fraud often take or cause to be taken photographs of themselves, their associates, their property, their stolen identities and/or counterfeit identity documents, and such items are usually maintained within their residence and sometimes on electronic devices such as cell phones.

e. *Shipping Records*: Based on my training and experience, individuals involved in identity fraud will often ship fraudulent identifications or PII via the United States

Postal Service or private mail carrier in order to distribute false identifications or PII to other co-conspirators. Shipping documents, records, and materials, to include commercial shipping packages, packaging materials, envelopes, stamps, commercial shipping/mailing labels, or items used to package identity documents, may help identify other co-conspirators and sources of stolen identification.

f. *Documents that show Indicia of Possession*: Where the identity of the named co-conspirators is still being confirmed, I would request permission to search for any documents or files, in any form, that show indicia of possession of the place or device to be searched: including articles of personal property, such as personal identification, immigration documents, personal correspondence, emails, delivery pouches, diaries, checkbooks, notes, photographs, keys, utility bills, receipts, personal telephone and address books or contact lists, and videos, tending to establish the identity of the person or persons in control of the areas to be searched;

101. *Cash or Cash Equivalents*: Similarly, in my experience, fraudsters will keep and retain the actual proceeds of identity theft, usually large amounts of currency (exceeding $500) or readily transported assets which are used as cash equivalents (e.g. cashiers' checks bearer's bonds, gold, diamonds, precious jewels, prepaid debit cards and gift cards).

102. *Instrumentalities*: Based on my training and experience, fraudsters may also keep instrumentalities of manufacturing fraudulent identity documents, to include printers, presses, seals, stamps, inks, dyes, specialty paper, templates, programs, hard drives, software programs, and packaging for the same in furtherance of their trade. These items are used to produce the false identifications which they need to further their criminal enterprise.

103. *Containers and Keys*: It is common for individuals who are involved in identity theft and financial fraud to store the records of those activities and proceeds of those activities in secure areas over which they have control such as safes, bags, locked drawers, briefcases, and duffel bags, among other locked containers, as well as on electronic devices such as cell phones. Additionally, keys for these storage facilities, businesses, locked containers, cabinets, safes, safe deposit boxes, conveyances and/or other residences would be relevant to establish ownership and control over any areas where evidence or instrumentality of criminal activity is kept and maintained.

104. *Written Correspondence or Other Information:* Based on my training and experience, often times co-conspirators will possess hard copies or electronic copies of communications between themselves and other as yet to be identified co-conspirators. This information could assist in identifying other co-conspirators, as well as the potential sources for stolen identities and PII. In addition, individuals involved in identity fraud will often draft correspondence to different establishments posing as a victim, making requests to change addresses, phone numbers, SIM cards, credit card information, financial data, background check services or loyalty program information in order to obtain further supporting PII and documents in furtherance of a fraudulent scheme. These documents would help identify historical and prospective victims of fraud, as well as *modis operandi* of the scheme itself.

TECHNICAL TERMS

105. Based on my training and experience, I use the following technical terms to convey the following meanings:

106. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio

signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

107. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

108. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large

amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

109. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

110. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

111. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

112. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

113. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

114. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

115. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as wireless telephones, digital cameras, portable media

players, GPS navigation devices, and PDAs. That is, devices like the Devices described in Attachment A have the ability to take, save, store, send, and receive photographs and videos, data, voice messages, text messages, e-mails, and other communications via messaging applications. Similar devices can also store information (including phone books/contact lists, calendars (including travel information), and call history (including incoming, outgoing, and missed calls); work with word-processing documents, spreadsheets, and presentations; perform different functions and save data associated with those functions via apps; and access the internet. I am also aware that devices like the nine Devices described in Attachment A typically have many of these abilities as well. Digital photographs, videos, and screen captures may contain evidence of additional victim identities or co-conspirators.

116. I also am aware that the Devices may contain relevant records and documents in digital format related to identification records, travel records, financial records, photographic records, shipping records, and indicia of possession or use documents. and other written communications (as previously described in this affidavit). These include but are not limited to records regarding identities, passport cards, checks, personal identifying information, and means of identification used, purchased, sold, shipped, created/made, counterfeited, forged, or possessed; financial transactions conducted (including means of conducting transaction, purpose of conducting transaction, date of transaction, location of transaction, individuals and accounts involved in transaction, details of transaction, amount and means of payment involved in transaction, and means of identification used in transaction); and amounts of money to be paid or collected or owed. Additionally, records that could show evidence of user attribution for each of the Devices may be maintained and visible on the phone, in the form of everything from subscriber and login data, to communications, to “selfies,” or photographs of the user of the Device.

117. I am also aware that the Devices may contain written communications and other information (as previously described in this affidavit), which includes but is not limited to call logs, text messages, voicemail messages, video and photo messages, messages drafted, sent or received via messaging applications, email messages

118. In my training and experience—including from the search of electronic devices seized in similar investigations—examining this data stored on devices of these types can uncover, among other things, evidence that reveals, suggests, or confirms who possessed or used each device. Such information may also serve as evidence of an agreement and association between and among those involved in criminal activities—including bank fraud, identity theft, false use of a passport, and other offenses—as well as evidence of specific instances of such conduct. Such information may also serve as evidence of an agreement and association between and among those involved in money laundering activities, as well as evidence of specific instances of conducting or attempting to conduct financial transactions involving proceeds of specified unlawful activities and the knowledge and intent of the individuals involved in those financial transactions. Based on my training and experience, electronic devices like the Devices have the capability to keep and maintain contact lists, including addresses, telephone numbers, and other contact lists such as names, addresses, phone numbers, or any other identifying information. In my experience, devices like the Devices can keep lists of customers, associates, victims, and potential victims and related PII in the same places as these address books. Therefore, the contact list information may contain information on other co-conspirators, including their true identities, as well as information about historical and prospective victims of identity fraud.

119. Based on my training, experience, and research, I know that individuals involved at all levels of these fraud rings regularly rely on cellular telephones for many purposes essential

to organizing their conspiracies and engaging in criminal conduct like bank fraud and aggravated identity theft. By DOWNS' admission, he utilized a cellular phone that was provided to him by his handlers, and he would use applications such as Telegram to communicate with his co-conspirators and handlers. Those uses include, among others, purchasing and sharing victims' PII and bank account information, checking victims' bank account balances, operational coordination, placing orders for counterfeit passport cards, taking and transmitting photographs to place on counterfeit passport cards, and recruiting "impostors" and other participants through social media. In this case, DOWNS stated that identifications were shared via the use of cellular telephones and messaging applications therein. I know that cellular telephones are regularly used to maintain contact and communication among conspirators through telephone calls, text and e-mail messages, and messaging applications (such as Telegram, WhatsApp, Signal, and Discord). Such devices are also used to save contact names and numbers for confederates and sources of supply (such as suppliers of PII and/or counterfeit forms of identification). In terms of coordinating operations, cellular telephones are frequently used to arrange and communicate regarding travel (like flights, vehicle rentals, accommodations) and send, receive, and store travel documents (like itineraries, reservations, receipts, tickets). Otherwise, innocuous communications like "I'm landing" or "pick me up at the terminal" may demonstrate or corroborate offenders' travel patterns and identify co-conspirators.

120. Based on my training, experience, and research, I know that GPS and other location information stored on devices like the Devices can serve as direct evidence of cellular telephones'—and thus, their owners'—presence at or near the scene of specific conduct but can also serve as evidence of intent or planning among co-conspirators by demonstrating locations in which various devices—and thus, their owners—are present at a given time and/or travel in

concert. For example, location information demonstrating travel by DOWNS or others to New Hampshire and/or other states would demonstrate or confirm such travel in concert and a common agreement and understanding. Location information may also assist in identifying other banks at which these individuals may have engaged in bank fraud and identity theft on other occasions or confirm their presence at or near those banks as additional conduct and victims are identified.

121. I have known intended recipients of, or those who cause other individuals to conduct, and those who conduct or are otherwise involved in financial transactions to communicate by cellular phone regarding those transactions, including to provide instructions on how to conduct a transaction, the individuals to whom a transaction should be directed or sent, and to request and provide verification or identifying information regarding attempted or completed transactions (such as receipts or photographs of the same).

122. Call logs, text messages, and other communications are important evidence regarding who a device's owner or user is in touch with, when such contact is made, and how often the contact occurs. Such information may assist in demonstrating a common understanding or agreement between the individuals involved in a conspiracy or fraud ring. Additionally, fraud- and money-laundering-related messages are often not explicit in nature but instead are veiled, coded, or non-specific. The content of a message, as well as the context provided by other messages in that conversation, can assist in identifying the meaning of such veiled or coded phrases. The use of such veiled or coded phrases may demonstrate a common understanding or agreement between individuals involved in a conspiracy or fraud ring.

123. Based on my training, experience, and research, I also know that those involved in conspiracies to commit bank fraud and/or identity theft commonly use multiple cellular telephones to compartmentalize different members of a conspiracy or organization and/or to avoid (or attempt

to avoid) electronic detection by law enforcement. It is also common for offenders to use cellular telephones registered in the names of others and/or pre-paid phones that do not require a registration name to be on file with a phone company to avoid being linked to the phones by law enforcement. Information regarding the telephone number assigned to or used by each of the Devices will assist me in identifying or confirming subscriber information—if it exists—and additional call detail records associated with the account to which that number is assigned.

124. Based on my training and experience, my involvement in this and other investigations, and information provided by other law enforcement agents who have investigated similar conduct, I know that searches of cellular telephones like the Devices have yielded evidence—including the items described in Attachment B—of contact and association between and among offenders engaging in the Subject Offenses and their associates. Such evidence may further establish an individual's intent to engage in the Subject Offenses and the actual commission of the Subject Offenses.

125. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the Subject Offenses described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when.

126. There is probable cause to believe that this forensic electronic evidence might be on the Devices because of the statements made by DOWNS related to the fraud scheme, as well as the general investigative knowledge which I have discussed relating to these fraud schemes.

127. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

128. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

129. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

130. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

131. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

132. *Manner of execution.* Because this warrant seeks only permission to examine property and Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

133. I submit that this affidavit supports probable cause for a search warrant authorizing the seizure and examination of the Target Vehicle and the Devices described in Attachment A to seek the records and information described in Attachment B.

Respectfully submitted,

/s/ Brian R. Gundersen
Brian R. Gundersen, Special Agent
U.S. Department of State
Diplomatic Security Service

Dated: 5/11/2024

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: May 13, 2024 /s/ Talesha L. Saint-Marc
Time: 12:03 PM HONORABLE TALESHA L. SAINT-MARC
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

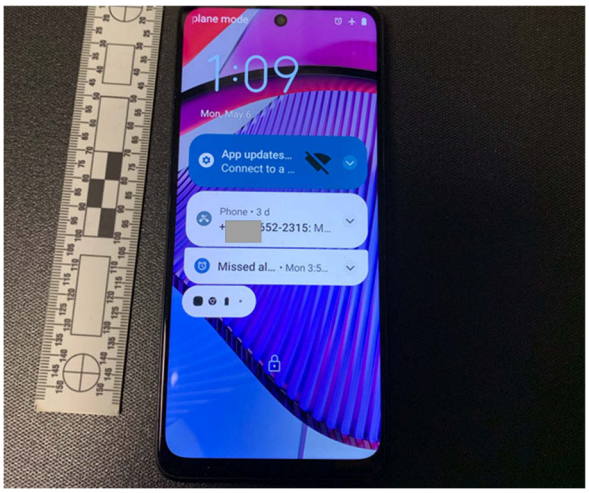
The property to be searched is the following:

1. The property to be searched is as follows:

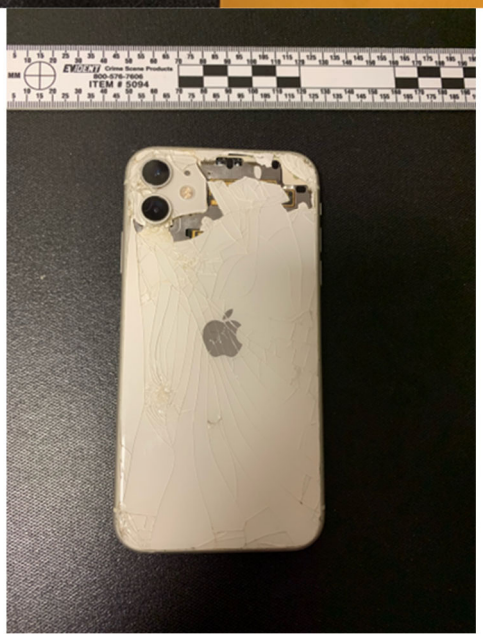
   a. A dark grey 2020 Jeep Cherokee, bearing Florida registration 24AUXR, registered to PV Holdings, d/b/a Avis Rental (Target Vehicle), a photograph of the rear of this vehicle is attached below:

b. A blue Samsung phone with no case assigned PPD Property No. 24-633-PR, recovered off the person of DOWNS (Device 1), photographs of the front and back of the device are attached below:

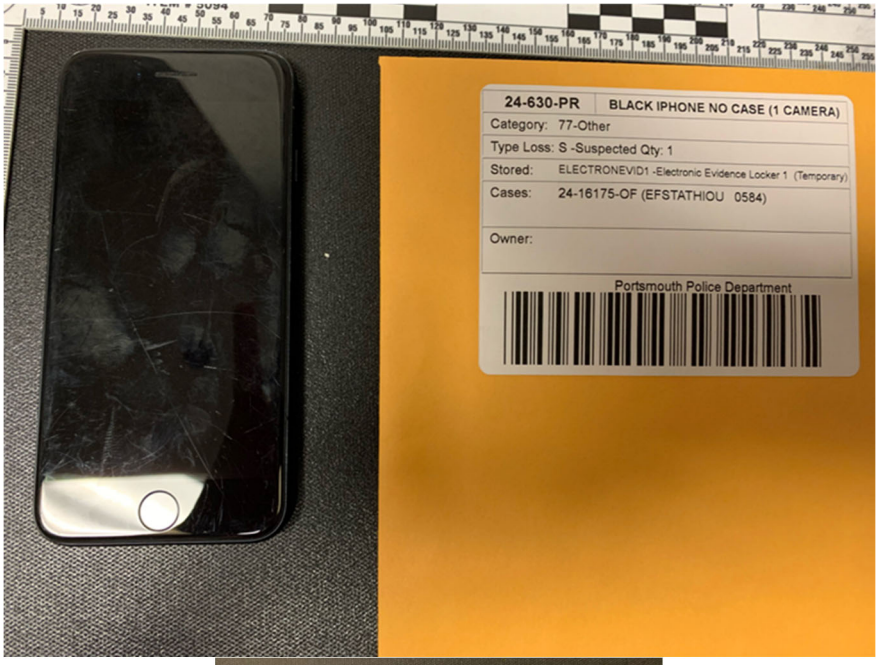

c. A black Motorola phone with no case assigned PPD Property No. 24-632-PR, recovered off the person of DOWNS (Device 2), photographs of the front and back of the device are attached below:



d. A white Apple iPhone with no case, broken back assigned PPD Property No. 24-631-PR, recovered from inside the TARGET VEHICLE in the front center console area between the area where CUNNINGHAM and NAAR were seated (Device 3), photographs of the front and back of the device are attached below:



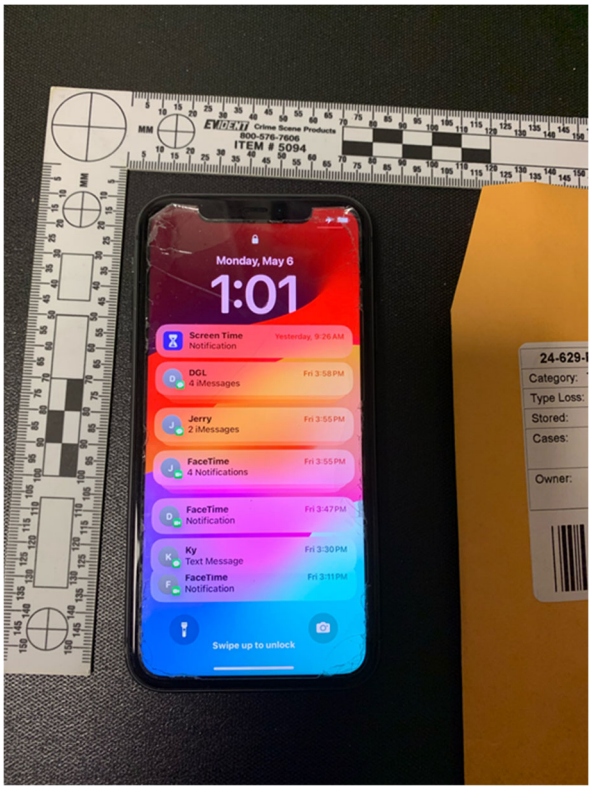
e. A black Apple iPhone with no case assigned PPD Property No. 24-630-PR, recovered from inside the TARGET VEHICLE in the front driver's side door panel next to where CUNNINGHAM was seated (Device 4), photographs of the front and back of the device are attached below:



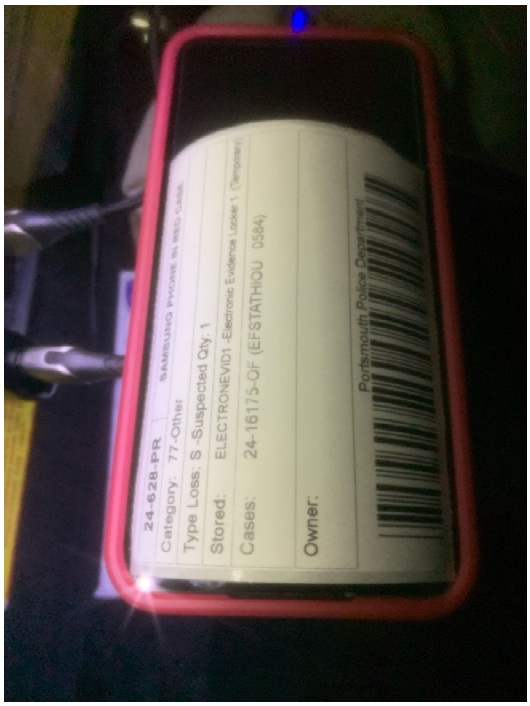
f. A white Apple iPhone with black Otterbox case assigned PPD Property No. 24-625-PR, recovered from inside of the TARGET VEHICLE and belonging to CUNNINGHAM who used this phone to look up an Avis rental agreement during the motor vehicle stop in the presence of PPD (Device 5), photographs of the front and back of the device are attached below:

g. A beige Apple iPhone with beige case assigned PPD Property No. 24-626-PR, recovered in the TARGET VEHICLE and belonging to NAAR, who was observed by PPD to be actively using this phone during the motor vehicle stop (Device 6), photographs of the front and back of the device are attached below:

h. A black Apple iPhone with no case assigned PPD Property No. 24-629-PR, recovered from inside the TARGET VEHICLE in the front center console area between the area where CUNNINGHAM and NAAR were seated (Device 7), photographs of the front and back of the device are attached below;



i. A black Samsung phone with red case assigned PPD Property No. 24-628-PR, recovered from inside the TARGET VEHICLE in the pocket behind the driver's seat, immediately in front of where STACK was seated (Device 8), photographs of the front and back of the device are attached below



j. A white Apple iPhone with no case, (Device 9) currently inside of the Target Vehicle on the front passenger seat where NAAR had been seated, a photograph of the device is attached below:

hereinafter, Devices 1, 2, 3, 4, 5, 6, 7, 8, and 9 will be collectively referred to as "the Devices."

ATTACHMENT B

Items to be Seized

1. Controlled substances;

2. Weapons to include firearms, ammunition, rifles, shotguns, privately manufactured firearms, explosive devices, silencers, magazines, Glock switches, targets, ballistic vests, etc., in which there is no immediate appearance of legitimate use;

3. Identification documents and information, in any form, pertaining to any names, as well as PII in any form pertaining to any names, including but not limited to PII recorded in writing or electronically, in written communications such as email, text or other social media platform, photographs, video and voice messages;

4. Electronic devices used to communicate with other imposters and/or handlers; including cellular telephones, pagers, and other electronic devices;

5. Records or information in any form pertaining to the possession, purchase, sale, manufacture, or disposition of fraudulent identification documents, to include those obtained through fraud or those manufactured, altered, or generated in digital form; any true or counterfeited Government-issued documents, to include passports, visas, driver's licenses, certificates, Social Security cards, or any other indicia of identity or citizenship;

6. Records or information in any form pertaining to air, sea, or ground travel into or within the United States, to include receipts, boarding passes, airline or other carrier documentation, hotel records, hotel keys, invoices, photographs, visas, visa supporting documents, or digital copies thereof;

7. Banking and financial records, in any form, as well as books, records, ledgers, journals, statements, receipts, invoices, billings, financial statements, balance sheets, notes and work papers concerning DOWNS, CUNNINGHAM, NAAR, STACK, and REDMOND, and any other names that they may be known by, business entities in which they are stakeholders, or co-conspirators; and materials evidencing expenditures of identity theft and bank fraud proceeds including, the purchase of large assets, including digital image storage devices, records of real estate or securities transactions, escrow files, wire transfer records, automobiles, motorcycles, trucks, or other vehicles purchased with cash or cash equivalents; credit and debit card records, including records of purchases, withdrawals, deposits and cash advances made with credit and debit cards, and including statements and receipts;

8. Photographs, negatives, video tapes, films, depicting the subjects of the investigation and their criminal associates, (showing association with the associates, depicting their assets or depicting stolen identities or counterfeit identity documents);

9. Records or information in any form pertaining to shipping, including shipping materials such as commercial shipping packages, packaging materials, envelopes,

stamps, commercial shipping/mailing labels, or items used to package identity documents;

10. Records or information in any form tending to show indicia of possession of the place or device to be searched: including articles of personal property, such as identification, any form of PII, immigration documents, personal correspondence, delivery pouches, diaries, checkbooks, notes, photographs, keys, utility bills, receipts, personal telephone and address books or contact lists, and videos, tending to establish the identity of the person or persons in control of the areas to be searched;

11. Large amounts of currency (exceeding $500) or readily transported assets which are used as cash equivalents (cashiers' checks, bearer bonds, gold, diamonds, precious jewels, etc.); prepaid debit cards and gift cards;

12. Instrumentalities of manufacturing fraudulent identity documents, to include printers, presses, seals, stamps, inks, dyes, specialty paper, templates, programs, hard drives, software programs, and packaging for the same;

13. Any safes, bags, locked drawers, briefcases, and duffel bags, among other locked containers, as well as on electronic devices such as cell phones. Additionally, keys for these storage facilities, businesses, locked containers, cabinets, safes, safe deposit boxes, conveyances and/or other residences to establish ownership and control over said containers;

14. Written correspondence to or from, documents, or other information in any form pertaining to or referencing communications between DOWNS, CUNNINGHAM, NAAR, STACK, and REDMOND, and any other names they may be known by, along with any other as yet to be identified co-conspirators, as well as any communications of any kind regarding any person changing their identity information, to include changes of address, phone number, telephone SIM card, credit information, financial data, background check services or retail loyalty program information;

22. For the Devices, I seek to search the telephones for the following information from January 1, 2024 to present:

a. the telephone number and other instrument numbers and subscriber numbers or identities assigned to/used by the Devices;
b. GPS and historical location data saved on the Devices;
c. Digital photos, screen captures, and videos saved on the Devices;
d. Call logs (including local and long-distance connection records and records of session times and durations), text-, photo- and video- messages, messages drafted, sent, or received via messaging applications; emails, voicemail messages of the Devices;
e. Address, telephone, and contact lists (including names, addresses, phone numbers, or any other PII) contained in the Devices;

f. Lists of customers, associates, victims, and potential victims and related identifying and contact information on the Devices (including names, addresses, phone numbers, or any other identifying information);
g. Business records, including word processing documents, spreadsheets, and presentations and applications associated with data retention, including browser search history;
h. Records in any form regarding identities, passport cards, checks, PII, and means of identification, used, purchased, sold, shipped, created/made, counterfeited, forged, or possessed; financial transactions conducted (including means of conducting transaction, purpose of conducting transaction, date of transaction, location of transaction, individuals and accounts involved in transaction, details of transaction, amount and means of payment involved in transaction, and means of identification used in transaction); and amounts of money to be paid or collected or owed;
i. Any other information related to sources of means of identification, PII, financial account information, and other information regarding victims and potential victims;
j. Personal calendar entries and travel logs (including any information recording schedules or travel, such as vehicle rentals, flights, transportation like cabs, Uber, or Lyft, and accommodations);
k. Any electronic bank records, checks credit card bills, account information, and other financial records; and
l. Any evidence of user attribution showing who used, controlled, or owned the device at the time the things described above were created, edited, deleted, or possessed, such as logs, phonebooks, saved usernames and passwords, documents, payment and delivery receipts, browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.